IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF MISSISSIPPI
OXFORD DIVISION

UNITED STATES OF AMERICA

v. CRIMINAL CASE NO. 3:21-cr-107-SA

JAMARR SMITH, THOMAS AYODELE,
and GILBERT MCTHUNEL DEFENDANTS

ORDER AND MEMORANDUM OPINION

On November 4, 2022, Jamarr Smith filed a Motion to Suppress [74]. Thomas Ayodele and Gilbert McThunel filed Joinders to the Motion [74]. *See* [76, 79]. The Defendants seek to suppress all evidence derived from the November 2018 geofence warrant which was used to identify them as suspects of a robbery that took place in February 2018. The Court held a hearing on the Motion [74] on January 31, 2023. Having considered the evidence presented at the suppression hearing, as well as the parties' filings and applicable authorities, the Court is prepared to rule.

Factual Background

The parties agree as to many of the underlying facts that led to the Indictment [1] being filed against the Defendants.

Around 5:25 PM on February 5, 2018, a U.S. Postal Service Highway Contract Route Driver, Sylvester Cobbs, was robbed as he was picking up mail from the Lake Cormorant Post Office, in Lake Cormorant, Mississippi. Cobbs' job as a driver consisted of picking up mail from the Dundee, Tunica, Robinsonville, Lake Cormorant, and Walls, Mississippi Post Offices and transporting mail to the Processing and Distribution Center in Memphis, Tennessee.

According to Cobbs, on the day in question, he was parked in the parking lot of the post office when he was approached from behind by an unknown African American male wearing a black long-sleeve shirt and a black ski mask who was approximately 5'9" to 6'0" tall. The man pointed a handgun at Cobbs with one hand and some form of mace with the other. The man then attempted to lock Cobbs inside the vestibule of the post office; however, Cobbs fought back with the man and the man pistol whipped Cobbs several times in return. After that, according to Cobbs, the man went to the back of the mail truck and took three registered mail sacks, which contained $60,706. The man also took Cobbs' post office keys. Thereafter, the man fled, and Cobbs drove his truck across the street to call his wife and postal management.

No suspect was arrested in connection to the robbery on the day of occurrence. However, in the following days, Postal Inspectors retrieved surveillance footage from a camera located at a nearby farm office. The camera captured the robbery on video. The video showed a red Hyundai (believed to be an Elantra) and a large white SUV (believed to be a newer model GMC Yukon XL) in the area. The video revealed the suspect getting out of the SUV before the robbery, and it is inferred that the suspect got back into the SUV before fleeing the scene. According to Todd Matney's (inspector of the United States Postal Inspection Service) affidavit in support of his search warrant application, the "Postal Inspectors conducted a detailed review of the video surveillance and it appears the robbery suspect is possibly using a cellular device both before and after the robbery occurs." [74], Ex. 2 at p. 4. Stephen Mathews (former Postal Inspector and supervisor of the Oxford, Mississippi Postal Inspector's Office) testified at the hearing that he interviewed Cobbs, who was unable to identify any suspects because the suspect was wearing a

ski mask.[1] Sometime after obtaining the video footage, but prior to applying for the warrant, Mathews located an eyewitness who lived across the street. According to Mathews, the witness asked the driver of the red Hyundai if he needed any help. The driver informed the eyewitness that he was looking for Highway 61. At this point in time, the witness was unable to identify the driver of the car.[2]

On November 8, 2018 (nine months after the robbery), Inspector Matney applied for a search warrant seeking information from Google to locate potential suspects and witnesses in connection to the February robbery. This specific type of warrant is known as a geofence warrant. According to Inspector Matney, he worked with Mathews, spoke with other investigators from other states who had applied for geofence warrants, and consulted with the United States Attorney's Office in Oxford, Mississippi before applying for the geofence warrant.

A geofence warrant is a fairly new investigative technique, wherein law enforcement request's location data from a third-party, such as Google. This type of warrant allows law enforcement to rely on technology to locate unknown potential suspects and witnesses of a crime. Attached to the Defendants' Motion to Suppress [74] is Spencer McInvaille's (the Defendants' expert) report which sets forth a three-step process that Google follows when responding to a geofence warrant. [74], Ex. 4.[3]

[1] For context, Mathews was the supervisor of the Postal Inspector's Office in Oxford, Mississippi in 2018—the time the warrant was applied for. At the time of the hearing, and currently, Mathews is no longer an active law enforcement officer. Therefore, the Court will hereinafter not refer to Mathews as an "Inspector."
[2] Mathews testified that after the three suspects were arrested (several months later), he presented the eyewitness with three separate photo lineups to see if the eyewitness could identify any of the suspects. Although the eyewitness was unable to identify McThunel or Smith in their respective lines, the eyewitness did identify Smith as the person he saw driving the red Hyundai.
[3] While the parties, to some extent, dispute the information returned from the geofence warrant in this case, the parties do not dispute the three-step process Google follows when it responds to a geofence warrant.

According to the report, a geofence warrant demands that Google search its database, known as the Sensorvault, to locate unknown suspects of crime. At the outset, law enforcement provides Google with geographical and temporal parameters around the time and place where the alleged crime occurred. The first step requires Google to search its Sensorvault for *all* users who have location history enabled at the time the warrant was executed. At the hearing McInvaille testified that, when acting in accordance with a geofence warrant, Google searches data for all users who had their location history enabled because the data itself is not capable of being stored in a way to search a specific area. Thus, Google searches all location history stored in its Sensorvault. Google describes the location history as a "[p]ersonal and private journal of the user's location." *Id.* at p. 1. To be clear, location history is not automatically enabled. A user must opt-in to sharing his or her location history either through phone set up or through an app.

After Google searches the Sensorvault and determines the accounts that were within the geographical parameters of the warrant, it returns to law enforcement a list giving each account an anonymized device ID, also including the date and time, longitude and latitude, the source, and the maps display radius. According to the report, "the maps display radius is indicated in meters and the radius is drawn around the center point referenced with the latitude and longitude" and "Google estimates the device should be located within the circle and states that their goal is for that to be true 68% of the time." *Id.* at 5. During the hearing, the Government introduced an exhibit illustrating this process, and McInvaille provided testimony explaining it in more detail.

Step Two is a request for contextual data. During this step, law enforcement reviews the anonymized list and determines which device IDs are relevant to the investigation. Then, law enforcement can request additional de-anonymized information that goes beyond the parameters of the initial geofence. According to Google, the purpose of this step is to potentially eliminate

false positives or determine if a device ID is relevant. *Id.* at p. 7. This step also allows law enforcement to compel Google (if authorized in the request) to provide account-identifying information, such as an email address, for the device IDs that law enforcement deems relevant.

In the third step, Google produces the subscriber's information for the accounts that were determined relevant in Step Two. This data is provided in a de-anonymized format which includes email addresses from Step Two, along with the names associated with the device IDs.

After the magistrate judge approved the warrant, Inspector Matney submitted the warrant to Google. Inspector Matney testified that, submitting the warrant to Google required him to access a legal portal and sign in with a government email address. After he signed in, Inspector Matney was able to upload the warrant and any subsequent documents through the portal.

Attached to the warrant was "Attachment A." Section II of the attachment outlined the three-step process that Inspector Matney submitted to the magistrate judge for his approval. Section II specifically provided:

> To the extent within the Provider's possession, custody, or control, the provider is directed to produce the following information associated with the Subject Accounts, which will be reviewed by law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of 18 U.S.C. section 2114(a), Robbery of a U.S. Postal Service Employee.
>
> 1. Location Information. All location data, whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, and Wi-Fi location, including the GPS coordinates, estimated radius, and the dates and times of all location recordings, between 5:00 p.m. CT and 6:00 p.m. CT on February 5, 2018;
> 2. Any user and each device corresponding to the location data to be provided by the "Provider" will be identified only by a numerical

> identifier, without any further content or information identifying the user of a particular device. Law enforcement will analyze this location data to identify users who may have witnessed or participated in the Subject Offenses and will seek any additional information regarding those devices through further legal process.
> 3. For those accounts identified as relevant to the ongoing investigation through an analysis of provided records, and upon demand, the "Provider" shall provide additional location history outside of the predefined area for those relevant accounts to determine the path of travel. This additional location history shall not exceed 60 minutes plus or minus the first and last timestamp associated with the account in the initial dataset. (The purpose of the path of travel/contextual location points is to eliminate outlier points where, from the surrounding data, it becomes clear the reported point(s) are not indicative of the device actually being within the scope of the warrant.)
> 4. For those accounts identified as relevant to the ongoing investigation through an analysis of provided records, and upon demand, the "Provider" shall provide the subscriber's information for those relevant accounts to include, subscriber's name, email addresses, services subscribed to, last 6 months of IP history, SMS account number, and registration IP.

[74], Ex 3 at p. 2.[4]

As this quoted language illustrates, the language of the warrant largely tracks Google's three-step process outlined above. After receiving the warrant, Google followed its three-step process. Although the precise number of user accounts searched is unclear, Google estimated that number to be around 592 million accounts at the time the warrant was executed. The warrant authorized an hour-long search from 5:00 PM to 6:00 PM on February 5, 2018. The geofence covered approximately 98,192 square meters around the Lake Cormorant Post Office. The warrant, consistent with Step Two, authorized law enforcement to obtain additional location history for a registered device "60 minutes plus or minus the first and last timestamp associated with the account

[4] Although this Section II information was not attached to the copy of the warrant attached to the Motion to Suppress [74], this appears to have been an oversight when the Motion [74] was initially filed. This issue was addressed at the hearing, and the Court has reviewed the official copy of the original warrant and notes that Section II *was* in fact part of the warrant.

in the initial dataset." *Id.* Google returned Step One information in April 2019. This step returned three device IDs (in an anonymized format) within the requested parameters (with two of the three devices registering multiple times). *See diagram below*. Inspector Matney testified that he then reviewed the device IDs to ensure they fell within the geofence coordinates.

Device ID	Date	Time	Latitude	Longitude	Source	Maps Display Radium (m)
1091610859	2/5/2018	17:22:45 (-06:00)	34.9044587	-90.2159436	WIFI	122
1091610859	2/5/2018	17:24:45 (-06:00)	34.9044587	-90.2159436	WIFI	98
1091610859	2/5/2018	17:27:04 (-06:00)	34.9044587	-90.2159436	WIFI	122
1091610859	2/5/2018	17:27:35 (-06:00)	34.9044587	-90.2159436	WIFI	104
1091610859	2/5/2018	17:28:06 (-06:00)	34.9044587	-90.2159436	WIFI	92
1091610859	2/5/2018	17:28:42 (-06:00)	34.9044587	-90.2159436	WIFI	146
1091610859	2/5/2018	17:30:56 (-06:00)	34.9044587	-90.2159436	WIFI	347
1353630479	2/5/2018	17:58:35 (-06:00)	34.9044587	-90.2159436	WIFI	110
1577088768	2/5/2018	17:22:27 (-06:00)	34.9040345	-90.2155529	GPS	11
1577088768	2/5/2018	17:24:04 (-06:00)	34.9042131	-90.2155945	GPS	18
1577088768	2/5/2018	17:25:08 (-06:00)	34.9045528	-90.2151712	GPS	37

At this point, the parties' versions of events diverge. The Defendants contend that, before receiving Step Two data, law enforcement did not follow the applicable Step Two narrowing measures. Instead, without obtaining an additional warrant (which the Defendants contend violated the "further legal process" language in the warrant), Inspector Matney and Mathews decided which device IDs were relevant and requested additional de-anonymized information for all three devices. Although, the Defendants, along with McInvaille, contend that it appeared Step Two had been skipped and it was not contained in discovery, Inspector Matney testified at the hearing that, in May 2019, he requested Step Two data through the portal. According to Inspector Matney, he, along with Mathews, decided that the device IDs ending in "859" and "768" were relevant because those devices registered multiple times within the geofence. They decided the third device ID, which only registered one time within the geofence, could have been a potential witness, but ultimately was not relevant to the investigation. Inspector Matney testified that on May 30, 2019,

Google sent law enforcement a letter containing Step Two data. There was also testimony that the Step Two narrowing measures took place with a subsequent warrant (discussed below) obtained in July 2019. During this step, according to the Government, Google also expanded the search to include the additional location history on the registered devices, as authorized in the warrant.

At the beginning of June 2019, Inspector Matney was injured, requiring a leave of absence from work, and Mathews took over as the lead investigator. Mathews testified that he received Step Three data around June 10, 2019. This data included de-anonymized information for *all* three devices IDs. The following email address were returned:

"2165781.Key.cvs",

"bleek2004.AccountInfo.txt",

"jamarrsmith33.AccountInfo.txt", and

"permanentwavesrecords.AccountInfo.txt."[5]

Through the information he received from Google, Mathews determined that the "jamarrsmith33.AccountInfo.txt" was Smith's email account and the "bleek2004.AccountInfo.txt" email account belonged to McThunel. At the hearing, Mathews testified that the email "permanentwavesrecords.AccountInfo.txt", which was associated with the third device, was deemed irrelevant to the investigation.

According to Mathews, he submitted another warrant (Google warrant) in the middle of July 2019. To be clear, this was *not* a geofence warrant, but instead sought location information as to those specific Google accounts that he had previously determined belonged to Smith and McThunel. Mathews testified that this warrant authorized specific location information connected

[5] Although this appears to be four separate email addresses, at the hearing, no reference was made to the "2165781.Keys.cvs" account. It is unclear to the Court what that email might reference. Nevertheless, it was clear at the hearing that the parties agree law enforcement only received de-anonymized information associated with three accounts—not four.

to Smith and McThunel's accounts and showed them traveling from Batesville, Mississippi to Lake Cormorant, Mississippi on the day of the robbery. Mathews also obtained phone records on all three suspects. The phone records revealed a 350 second phone call between Smith and McThunel during the time of the robbery. The phone records also indicated a phone call between Ayodele and McThunel, which is how Ayodele was identified as a third suspect.

Ultimately, the Government was able to identify the three Defendants and obtain an Indictment [1] against them. In the Motion to Suppress [74], the Defendants argue that the geofence warrant was invalid from its inception because it lacked probable cause and particularity. The Defendants also take the position that they had a reasonable expectation of privacy in their location history and that the geofence warrant violated that reasonable expectation. Furthermore, the Defendants argue that, in the event that the warrant was valid, the Government did not undertake "further legal process" to obtain additional information from Google as it said it would do, which made Steps Two and Steps Three of the search warrantless and illegal. Finally, they argue that the good faith exception set forth in *United States v. Leon*, 468 U.S. 897, 104 S. Ct. 3405, 82 L. Ed. 2d 677 (1984) does not excuse the defects of the warrant. They contend that the exclusionary rule should apply and that all the evidence seized constitutes "fruit of the poisonous tree."

Applicable Standard

"The defendant challenging a search must show the warrant to be invalid by the preponderance of the evidence." *United States v. Richardson*, 943 F.2d 547, 548 (5th Cir. 1991) (citing *United States v. Osborne*, 630 F.2d 374, 377 (5th Cir. 1980)). "That burden includes establishing standing to contest the evidence, and showing that the challenged government conduct constitutes a Fourth Amendment search or seizure." *United States v. Turner*, 839 F.3d 429, 432

(5th Cir. 2016). However, "when the government searches or seizes a defendant without a warrant, the government bears the burden of proving by a preponderance of the evidence, that the search or seizure was constitutional." *United States v. Guerrero-Barajas*, 240 F.3d 428, 432 (5th Cir. 2001).

Analysis and Discussion

The Fourth Amendment assures the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. Moreover, "no warrants shall issue, but upon probable cause, supported by oath and affirmation, and particularly describing the place to be searched, and the persons or thing to be seized." *Id.* The Fourth Amendment requires that a search warrant be issued only when there is probable cause to believe that an offense has been committed and that evidence exists at the place for which the warrant is requested. *United States v. Place*, 462 U.S. 696, 701, 103 S. Ct. 2637, 2641, 77 L.Ed.2d 110 (1983). If a warrant is invalid, the appropriate remedy is to suppress the evidence obtained through an unreasonable search or seizure. *United States v. Beaudion*, 979 F.3d 1092, 1097 (5th Cir. 2020).

As noted above, the Defendants raise several arguments as to the purported unconstitutionality of the geofence warrant and, consequently, the inadmissibility of the evidence obtained therefrom. Specifically, the Defendants contend they had a reasonable expectation of privacy in their data obtained through the warrant, the warrant lacked probable cause and particularity, and that the good faith exception is inapplicable. The Court will address the issues in turn.[6]

[6] The Court notes that, in its Response [87], the Government raised an argument that the Defendants' lacked standing. The Government did not raise this issue at the hearing and, perhaps, concedes this point. Nevertheless, the Court does not find the argument persuasive, as it is undisputed that the location history of both Smith and McThunel was obtained through the execution of the geofence warrant. Therefore, they have standing.

A. Reasonable Expectation of Privacy

Beginning first with the issue of reasonable expectation of privacy, the Defendants contend that they possessed a reasonable expectation of privacy in their location history. The Defendants rely on *Carpenter v. United States*, wherein the Supreme Court specifically rejected the application of the third-party doctrine on the basis that, given the unique nature of cellphone data, users do not truly voluntarily share their data with a third party. 138 S. Ct. 2206, 2220, 201 L. Ed. 2d 507 (2018). On the other hand, the Government takes the position that because a user voluntarily opts-in to sharing his location history they maintain no reasonable expectation of privacy. The Government further contends that obtaining two hours of the Defendants' location history is not the same as the seven days' worth of information obtained in *Carpenter* (which the Supreme Court later determined violated the defendant's reasonable expectation of privacy).

Other district courts have grappled with the privacy concerns that geofence warrants raise. The District Court for the Eastern District of Virginia, analyzing the constitutionality of a geofence warrant, declined to delve too deeply into the issue of whether the defendant possessed a reasonable expectation of privacy in his location history data obtained through the geofence warrant because the court found that the good faith exception applied. *United States v. Chatrie*, 590 F. Supp. 3d 901, 925 (E.D. Va. 2022). Although the *Chatrie* court did not reach a determination on the reasonable expectation of privacy issue, the court acknowledged its deep concerns with geofence warrants and stated that the "[c]urrent Fourth Amendment doctrine may be materially lagging behind technological innovations." *Id.* Most recently, the District Court for the District of Columbia followed the *Chatrie* court's reasonable expectation of privacy analysis. *United States v. Rhine*, 2023 WL 372044, at *28 (D.D.C. Jan. 24, 2023). Recognizing the novelty

of warrants of this nature and for reasons set forth more fully hereinafter, the Court need not definitively resolve that issue.

B. Probable Cause

Next, the Defendants contend that the geofence warrant is wholly invalid because it lacked sufficient probable cause. The Supreme Court has held that probable cause requires a "[f]air probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238, 103 S. Ct. 2317, 2332, 76 L. Ed. 2d 527 (1983). Furthermore, a warrant must not be overbroad. *United States v. Sanjar*, 853 F.3d 190, 200 (5th Cir. 2017) (citing *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 702 (9th Cir. 2009)). This requires probable cause to seize the particular things named in the warrant. *Id.* More specifically, the Fourth Amendment requires "that (1) a warrant provide sufficient notice of what the agents may seize and (2) probable cause exists to justify listing those items as potential evidence subject to seizure." *Sanjar*, 853 F.3d at 200 (citing *William v. Kunze*, 806 F.2d 594, 598-99 (5th Cir. 1986)).

The Defendants contend that the geofence warrant was not supported by probable cause because the warrant was overbroad. Specifically, the Defendants argue that the warrant did not identify any suspects and that the Government only learned the identity of the suspects via inverted probable cause. In their Memorandum [75], as well as at the hearing, the Defendants maintained that their probable cause argument was synonymous to *Ybarra v. Illinois*, 444 U.S. 85, 100 S. Ct. 338, 62 L. Ed. 2d 238 (1979), wherein the Supreme Court struck down a search warrant because although "the police did have probable cause to search the tavern where [Ybarra] happened to be when the warrant was executed, [] a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." 444 U.S. 85, 86, 100 S. Ct. 338, 339, 62 L. Ed. 2d 238 (1979). Although *Ybarra* addresses the physical

search of a person, the Defendants contend that the search of the tavern in *Ybarra* is synonymous to a search of Google's Sensorvault.

Conversely, the Government contends that Inspector Matney's affidavit in support of the warrant application contained more than enough information to establish probable cause. Particularly, the affidavit established that unknown suspects aided and abetted each other in committing the robbery. The affidavit also established a connection between Google location information and smartphones. Additionally, though the Government does not believe it was necessary, the affidavit stated that an unknown person was *possibly* using a cellphone before and after the robbery. Therefore, the Government contends that the affidavit included enough information to establish probable cause.

To aid its probable cause analysis, the Court considers the reasoning from *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345 (N.D. Ill. 2020) ("*Google III*"). There, the Government applied for a geofence warrant to investigate a series of arsons. *Id.* at 351. The geofence covered only a 15–30 minute time frame and only included the location of the arson sites, while excluding any irrelevant residential or commercial buildings. *Id.* at 357-58. The court concluded that the Government satisfied any overbreadth concerns by ensuring probable cause for location data on the suspects through "[o]n-site investigation, open source searches, and surveillance footage." *Id.* at 359. The magistrate judge determined that the warrant established sufficient probable cause and was not overbroad because the geofence only focused on the arson sites and structured geographical and temporal limitations in a manner to minimize capturing location data for uninvolved individuals. *Id.* at 357. The *Google III* court also noted that it was not necessary that

the affidavit contain information that the suspect possessed a phone during the commission of the crime to retrieve cellphone data. *Id.* at 355.

To further support its argument, the Government relies on *In re Search of Info. that is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d 62 (D.D.C. 2021) ("*Google V*"). In *Google V*, the Government applied for a geofence warrant around a building where the Government alleged federal crimes had occurred. *Id.* at 72. The geofence only covered a portion of the front half of the building and did not include any other structures. *Id.* The geofence was approximately 875 square meters. *Id*. The district court concluded that the warrant established sufficient probable cause because "[t]here [was] a fair probability that the search of Google's servers [would] uncover useful evidence—i.e., the identities of the suspects inside the [building]". *Id.* at 77. Further, there was evidence that the suspects were using their cellphones while inside the building. *Id.* at 78. The court ultimately concluded that because the geofence was tailored to the building the location information that Google would return would not include an unnecessarily broad number of uninvolved individuals. *Id.* at 80.

Against this backdrop, the Court turns to the facts of this case. Although the parameters of the geofence were relatively large in scope, the geofence was in a rural area where it was unlikely to return a large number of Google accounts. Moreover, the affidavit contained additional evidence that the suspect was possibly using a phone, and this Court agrees with Inspector Matney's characterization that the suspect was *possibly* using a phone. Although the Court makes no definitive determination as to whether the evidence of cellphone use is necessary, the Court finds, based on the facts of this case, that the statement aided the Government in establishing probable cause. The affidavit also established a connection between smartphones and Google. The

Government established sufficient probable cause that indicated Google possessed data that would reveal suspects of the robbery.

In essence, the Defendants' argument on this point seems to be a contention that geofence warrants in general violate the Fourth Amendment. The Court declines to make such a sweeping determination.

The Court finds that the geofence warrant contained sufficient probable cause. To the extent the Defendants' Motion [74] seeks suppression on that basis, it is DENIED.

C. Particularity

A search warrant must describe the items to be seized "[w]ith sufficient particularity such that the executing officer is left with no discretion to decide what may be seized." *Kunze*, 806 F.2d at 598 (citing *Marron v. United States*, 275 U.S. 192, 196, 48 S.Ct. 74, 72 L.Ed 231 (1927)).

The Defendants argue that the geofence warrant lacked particularity because it was not particular in the places to be searched or things to be seized. In their Motion [74], as well as at the hearing, the Defendants raise two arguments as to the particularity requirement. First, the Defendants argue that the geofence warrant failed to identify any particular suspects and that the magistrate judge would have never signed off on the warrant had he known it included a search of 592 million Google accounts. Second, the Defendants contend that the Government obtained additional information and decided which accounts to search in Steps Two and Three of Google's process and did so without obtaining an additional warrant, as required by the "further legal process" language in the warrant. Conversely, the Government contends that the warrant was tailored to the investigation and "[w]as narrowly constrained based on location, date, and time." [87] at p. 15. Moreover, as articulated by the Government, the warrant only sought location history for a total of two hours and was only searching for "[i]ndividuals present at the site of the robbery." [87] at p. 15. The Government further contends that the initial geofence warrant did not require

the agents to go back to the Court to obtain an additional warrant for Steps Two and Three. Instead, according to the Government, the phrase "upon demand", which is included in the warrant, meant upon the request from law enforcement and constituted the "further legal process" required under the warrant.

To support their particularity argument, the Government relies on the rationale from *United States v. James*, 2019 WL 325231 (D. Minn. Jan. 25, 2019.) In *James*, the Court authorized law enforcements use of cellphone "tower dumps" to locate suspects of a robbery. *Id*. at *1. The Court ultimately upheld the use of tower dumps because, through geographical and temporal parameters, the warrant was particular to the information sought. When asked about the difference between cellphone tower dumps and Google location history during the hearing, McInvaille explained that tower dumps provide data restricted to the location of the towers, whereas location history is stored in a way that requires Google to search *all* location history and not just a specific area. In other words, for a tower dump, the search can be limited to users in close proximity to a particular tower, whereas that same limitation cannot be accomplished in connection with a geofence warrant.

The Court again relies on *Google III* and *Google V*. In *Google III*, the magistrate judge found that the warrant met the particularity requirements because it narrowly identified the place to be searched by time and location limitations. *Google III*, 479 F. Supp 3d at 357. As noted above, the geofence only included a 15-30 minute timeframe and excluded residences and commercial buildings. *Id.* The *Google V* court reached the same conclusion for similar reasons. *Google V*, 579 F. Supp. 3d at *80. The district court found that the geofence contained sufficient temporal and geographic windows for the location data that was being sought. *Id.*

The Court notes the *Rhine* court (the most recent decision deciding the constitutionality of geofence warrants) also concluded that the geofence warrant at issue in that case met the particularity requirements. *Rhine*, 2023 WL 372044 at *32.

Here, the initial time period authorized by the warrant was limited to one hour and only authorized the retention of additional location history for a 60 minute time period for registered devices. The geofence encompassed the area in which the crime occurred. Furthermore, the affidavit specifically includes the latitude and longitude coordinates of where the crime occurred and states that "this application seeks authority to collect certain location information related to Google Accounts that were located within the Target Area during the Target Time Period." [74], Ex. 2 at p. 6. Simply put, this geofence contained similar temporal restrictions to the geofence warrants in *Google III* and *Google V*. The Court notes the stark difference in the geographical ranges of the geofence in *Google V* and the one presently before the Court. Here, the geofence is 98,192 square meters—a drastically larger difference than the 875 square meter geofence in *Google V*. However, considering that the geofence in the case at bar was in a rural area where there was an unlikely chance that a substantial number of uninvolved people would be captured in the geofence, the geographical size of the geofence does not cause this Court great concern.

In making that determination, the Court again finds it necessary to provide a qualification. The Court's determination on that point should not be interpreted as a determination that a geofence of 98,192 square meters is always permissible. In fact, there may very well be circumstances where it is not. The Court's determination is limited to the facts at issue here. A case-by-case analysis is appropriate.

Therefore, for reasons set forth above, the Court does not find the Government's tower dump argument directly on point, but does agree with the Government's overall position that the warrant was particular in identifying the places to be searched and things to be seized.

Next, the Defendants argue that, by not obtaining an additional warrant before obtaining additional information in Steps Two and Three, law enforcement did not comply with the "further legal process" language contained in the warrant. Therefore, the Defendants assert that the information obtained from Steps Two and Three is not particular. The court in *Google II* emphasized that "a warrant that meets the particularity requirement leaves the executing officer with no discretion as to what to seize." *Google II*, 481 F. Supp. 3d 730, 754 (N.D. Ill. 2020). There, the warrant did *not* require law enforcement to obtain an additional warrant for Steps Two and Three. *Id.* Therefore, the *Google II* court rejected the Government's particularity argument on the basis that the warrant was not narrowly tailored in a manner justified by the investigation. *Id.* In *Google V*, the magistrate judge reasoned that the warrant was valid because it required law enforcement to obtain further authorization from the court before receiving de-anonymized information on the Google accounts at Step Two. *Google V*, 579 F. Supp. 3d at 87. The *Google V* court further held, that any overbreadth concerns would be cured in the additional warrant obtained prior to receiving Step Two data. *Id.* Other Courts have criticized the lack of a requirement for additional authorization as providing law enforcement unbridled discretion. *See Google I*, 2020 WL 5491963 at 6; *Google II*, 481 F. Supp. 3d at 746; *Chatrie*, 590 F. Supp. 3d at 927.

Here, the Court finds that law enforcement did not follow the narrowing measures set forth in Step Two of Google's process. In fact, testimony from the hearing indicated that law enforcement did not narrow their investigation until the subsequent July 2019 warrant was obtained. This was a clear failure to follow the narrowing measure outlined in Step Two. Moreover,

without further authorization from the Court, Inspector Matney and Mathews chose which device IDs were of interest. During the hearing, McInvaille testified that Step Two of Google's approach was a narrowing measure that, without further authorization from a judge, gave law enforcement the discretion to choose which accounts were relevant. According to the Defendants, this cuts against the plain language contained in the warrant where it states that law enforcement "[w]ill seek any additional information regarding those devices through further legal process." [74], Ex. 3 at p. 2. On the other hand, the Government argued that further legal process was "upon demand" from law enforcement, not an additional warrant from the Court. In other words, the Government takes the position that "further legal process" was outlined in the later parts of Section II of Attachment A to the Warrant. Inspector Matney and Mathews additionally testified that they interpreted the "further legal process" language to mean that Google would produce additional information "upon demand" from law enforcement because the magistrate judge had already signed off on the initial warrant that included all three steps. To support that belief, Mathews testified that he resubmitted "Attachment A" (which was submitted along with the original warrant) instructing Google to comply with paragraph three of the attachment which states, "[a]nd upon demand, the 'Provider' shall provide additional location history. . ." [74], Ex 3. at p. 2.

As an initial matter, the Court disagrees with the Government's interpretation of the "further legal process" language. Furthermore, it was admitted at the hearing that the Government did in fact receive de-anonymized information for *all three* device IDs—even though, in its Response [87], as well as at the hearing, the Government maintained the position that only two of the device IDs were relevant to their investigation.

Although the Court rejects the Government's interpretation of the "further legal process" language, the Court does not question the credibility of Inspector Matney's nor Mathews'

testimony on that issue. In other words, the Court concludes that Inspector Matney and Mathews made a good faith interpretation that the "further legal process" language did not require them to return to the Court for an additional warrant before receiving Steps Two and Three data.

At the hearing, McInvaille testified that the "further legal process" language has shown up in other warrants and when it has, courts have interpreted that to mean that law enforcement must return to the court for authorization between each step of the Google process. He provided specific examples of other cases.

Ultimately, the Court makes no determination as to whether geofence warrants are per se constitutional but, instead, finds that a case-by-case determination is appropriate in determining the appropriate geographic parameters. In reaching its conclusion, the Court notes, and the parties agreed at the hearing, that in November 2018, the time law enforcement applied for the geofence warrant, there was no published case law on the constitutionality of geofence warrants. The Court finds that fact—and the novelty of geofence warrants as a whole, particularly at the time of Inspector Matney and Mathews' relevant conduct—to be important in analyzing this case.

The Court rejects the Defendants' argument that the warrant was so overbroad as to render it unconstitutional. But the Court does find that "further legal process" required law enforcement to obtain an additional warrant before requesting Steps Two and Steps Three data. The Government admits that no such warrant was obtained. Consequently, the critical determination becomes whether that failure warrants suppression or, as the Government contends, the good faith exception should apply.

D. Good Faith Exception

"The good faith exception to the exclusionary rule provides that 'evidence obtained during the execution of a warrant later determined to be deficient is nonetheless admissible if the executing officer's reliance on the warrant was objectively reasonable and made in good faith.'"

United States. v. Massi, 761 F.3d 512, 525 (5th Cir. 2014) (citing *United States v. Woerner*, 709 F.3d 527, 533 (5th Cir. 2013)) (additional citation omitted). "Applying the good-faith exception does not resolve whether a constitutional right has been violated; it simply is a judicial determination that exclusion of evidence does not advance the interest of deterring unlawful police conduct." *Id*. (citing *Leon*, 468 U.S. at 906-07, 104 S. Ct. 3405; *Gates*, 462 U.S. at 223, 103 S. Ct. 2317). "In effect, the good-faith exception limits the remedy of exclusion where the marginal or nonexistent benefits produced by suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion." *Id.* (citing *Leon*, 468 U.S. at 922, 104 S.Ct. 3405).

In *Leon*, the Supreme Court articulated four circumstances where the good faith exception does not apply: "1) when the issuing magistrate was misled by information in an affidavit that the affiant knew or reasonably should have known was false; 2) when the issuing magistrate wholly abandoned his judicial role; 3) when the warrant affidavit is so lacking in indicia of probable cause as to render official belief in its existence unreasonable; and 4) when the warrant is so facially deficient in failing to particularize the place to be searched or things to be seized that executing officers cannot reasonably presume it to be valid." 468 U.S. at 899, 104 S. Ct. 3405. The good faith exception analysis is focused on "[w]hether a reasonably well-trained officer would have known that the search was illegal despite the magistrate's authorization." *United States v. Payne*, 341 F.3d 393, 400 (5th Cir. 2003) (citing *Leon*, 468 U.S. at 922 n. 23, 104 S. Ct. 3405).

The Defendants contend that the good faith exception is not implicated here because three of the four circumstances articulated above are applicable. The Government disagrees and contends that the good faith exception should apply. Particularly, the Government relies on two

separate arguments on this point—first, under the holding from *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018); and second, from the traditional good faith exception articulated in *Leon*.

First, the Defendants contend that the good faith exception does not apply because the affidavit contained a misrepresentation that Inspector Matney knew or should have known was false. The Defendants base this argument on the rationale set forth in *Franks v. Delaware*, 438 U.S. 154, 98 S. Ct. 2674, 57 L. Ed. 2d 667. To prove this claim under *Franks*, the Defendants must show that (1) the affidavit supporting a warrant contained false statements or material omissions; (2) the affiant made such false statements or omissions knowingly and intentionally or with reckless disregard for the truth; and (3) the false statements or material omissions were necessary to the finding of probable cause. *Davis v. Hodgkiss*, 11 F.4th 329, 333 (5th Cir. 2021) (citing *Franks*, 438 U.S. at 155-56, 98 S. Ct. 2674) (additional citations omitted).

The portion of the affidavit in question, which ultimately, at least in part, led to the issuance of the geofence warrant, states that "Postal Inspectors conducted a detailed review of the video surveillance and *it appears the robbery suspect is possibly using a cellular device both before and after the robbery occurs.*" [74], Ex. 2 at p. 4. (emphasis added). The Defendants contend they meet the first two prongs of the *Franks* analysis because the video footage does not show a cellphone, making Inspector Matney's statement intentionally reckless. According to the Defendants, a more accurate statement would have read that "[i]t *does not* show the robbery suspect using a cellular device before or after the robbery occurs." [75] at p. 12. (emphasis added). Because of this, the Defendants argue that the statement is reckless.

At the hearing, Inspector Matney testified that there were several times during the video where the assailant's body language appeared to be consistent with talking on the phone. First, around the 6:50 minute mark. During this time, the assailant's arm appeared to be raised up to his

left ear for several minutes. Next, around the 13:34 minute mark, the assailant is seen crouching on the ground and making a movement that Inspector Matney believed was consistent with sending or checking a text message.

After reviewing the video footage and testimony from the hearing, the Court rejects the Defendants' argument that Inspector Matney stating the assailant is possibly using a cellphone is outright false. Although there is never a cellphone shown on the video, the Court finds the statement was not a misrepresentation and that Inspector Matney's interpretation of the video could have led him to believe that the assailant's body language was consistent with using a cellphone. The Defendants' contentions as to the language they would have preferred Inspector Matney to have used are unavailing. The Court does not find that Inspector Matney made a knowing misrepresentation.

Next, the Defendants argue that the good faith exception is not applicable because the warrant lacked probable cause and the warrant was facially deficient because it did not meet the particularity requirements. In its analysis above, the Court has already concluded that there was sufficient probable cause and that the particularity requirement was met. The Court sees no need to recite that analysis again and will not address those issues any further.

Ultimately, the Court finds the Fourth Circuit's reasoning in *McLamb* persuasive. In *McLamb*, the Fourth Circuit declined to find a warrant facially deficient when law enforcement faced with novel investigative techniques consulted with counsel prior to applying for a warrant. *McLamb*, 880 F.3d at 691. Here, included in the affidavit, Inspector Matney stated that he had conversations with other law enforcement officers before submitting the geofence warrant. In its Response [87], the Government also states that Inspector Matney consulted with the United States Attorney's Office prior to submitting the warrant. Inspector Matney's testimony on this point was

consistent with the Government's contention. Furthermore, throughout the hearing, it became abundantly clear that neither Inspector Matney nor Mathews had personal experience with geofence warrants when they applied for the present warrant. They both explained multiple steps that they took to attempt to undertake the inspection properly—such as consulting with an Assistant United States Attorney, communicating with other agencies across the country, and reviewing similar warrant templates. The Court found their testimony to be credible insofar as it concerned the steps they believed they were required to take in connection with the geofence warrant. Inspector Matney's testimony on this point was consistent with the Government's contention.

The Court also finds noteworthy the rationale underlying the good faith exception. *See Herring v. United States*, 555 U.S. 135, 145, 129 S. Ct. 703, 172 L.Ed.2d 496 (2009) ("To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it. . ."). Here, the Court struggles to see any wrongful conduct to deter. Before seeking the warrant, Inspector Matney and Mathews consulted with the United States Attorney's Office and sought legal guidance, and the Court finds credible their testimony that they believe the warrant did not mandate that they return to the Court for an additional warrant. Ultimately, the conduct of law enforcement in this case seems reasonable and appropriate when considering the specific circumstances with which the investigators were faced.

Although the Court's ruling today will certainly create clear authority as to the meaning of "further legal process," Inspector Matney and Mathews, at the time they sought the warrant and acted in accordance with it, did not have any authority upon which to rely. In fact, counsel for both parties conceded that there was no published authority on this issue at the time. Even today, the

case law is sparse. Ultimately, the Court simply does not find that suppression in this case would further the rationale underlying the good faith exception.

Conclusion

For reasons set forth above, the Motion to Suppress [74] is DENIED.

SO ORDERED, this the 10th day of February 2023.

/s/ Sharion Aycock
UNITED STATES DISTRICT JUDGE